

**Appln No. 09/833,969**  
**Amdt date March 31, 2006**  
**Reply to Office action of January 6, 2006**

**REMARKS/ARGUMENTS**

The Examiner rejected claim 3 under 35 U.S.C. 102(e) as being allegedly anticipated by Geiger, and claims 5, 7-9, 13-15, 27 and 28 under 35 U.S.C 103(a) as being allegedly unpatentable over Geiger in view of Strunk. In response, base claims 3 and 5 have been amended. Claims 3-5, 7-15 and 18-28 are pending in the application, of which claims 4, 10-12 and 18-26 are withdrawn.

Claim 3 is rejected under 35 U.S.C. 102(e) as being anticipated by Geiger. Claim 3, as amended specifies "receiving from the user an access list of possible requesters of the data and the additional data; storing the access list of possible requesters of the data and the additional data in the user-specific space; and providing the data indicative of the location of the user and the additional data regarding the user to possible requesters on the access list."

Regarding prior claim 3, the Office action refers to col. 4, lines 26-40 and lines 57-66 of Geiger to indicate that Geiger teaches "receiving an access list of possible requesters of the data in the user-specific space and providing the data indicative of the location of the user to possible requesters on the access list." Office action, page 3. The cited section of Geiger states that "on receipt of the location access permission attribute certificate, the requesting entity 25 establishes communication with the location server 21, for example by establishing a TCP/IP data or Secure Sockets Layer (SSL) connection, and sends the location access permission attribute certificate to the location server 21 with the request for the location of the mobile device." The cited section of Geiger further states that "the location server 21 verifies the location access permission attribute certificate received via the requesting entity 25 from the mobile device 15. This certificate is validated by verifying (as described above) the digital signature of the mobile device using the certification key that is common to both the location server 21 and the mobile device 15. If verification is successful in step 64, the location server 21 sends the location information to the requesting entity 25."

Thus, it does not appear that the cited portion of Geiger discloses or suggests "receiving from the user an access list of possible requesters of the data and the additional data; storing the

**Appln No. 09/833,969**  
**Amdt date March 31, 2006**  
**Reply to Office action of January 6, 2006**

access list of possible requesters of the data and the additional data in the user-specific space; and providing the data indicative of the location of the user and the additional data regarding the user to possible requesters on the access list," as specified in claim 3.

Accordingly, claim 3 is allowable over Geiger and the other cited art.

Claim 5 is rejected under 35 U.S.C 103(a) as being unpatentable over Geiger in view of Strunk. Claim 5, as amended specifies "the application server is further configured to store information received from and concerning an individual associated with the PCD in the user specific data space, the stored information in the user specific data space including an access list of possible requesters of information concerning the individual associated with the PCD, the access list being received from the individual associated with the PCD." In contrast, Geiger does not disclose or suggest the noted elements of claim 5.

Geiger states at col. 4, lines 26-40 that "on receipt of the location access permission attribute certificate, the requesting entity 25 establishes communication with the location server 21, for example by establishing a TCP/IP data or Secure Sockets Layer (SSL) connection, and sends the location access permission attribute certificate to the location server 21 with the request for the location of the mobile device." Geiger further states at col. 4, lines 57-66 that "the location server 21 verifies the location access permission attribute certificate received via the requesting entity 25 from the mobile device 15. This certificate is validated by verifying (as described above) the digital signature of the mobile device using the certification key that is common to both the location server 21 and the mobile device 15. If verification is successful in step 64, the location server 21 sends the location information to the requesting entity 25."

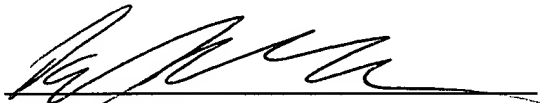
Thus, it does not appear that Geiger discloses or suggests "the application server is further configured to store information received from and concerning an individual associated with the PCD in the user specific data space, the stored information in the user specific data space including an access list of possible requesters of information concerning the individual associated with the PCD, the access list being received from the individual associated with the PCD," as specified in claim 5.

**Appln No. 09/833,969**  
**Amdt date March 31, 2006**  
**Reply to Office action of January 6, 2006**

Accordingly, claim 5 is allowable over Geiger in view of Strunk, as are dependent claims 7-9, 13-15, 27 and 28.

Accordingly, the application is in condition for allowance and allowance of same is respectfully requested.

Respectfully submitted,  
CHRISTIE, PARKER & HALE, LLP

By   
Daniel M. Cavanagh  
Reg. No. 41,661  
626/795-9900

SM/bl

RMW IRV1094816.1-\* -03/31/06 11:29 AM